Qudit Lifted Product Codes with Good Parameters

Lalitha Vadlamani, IIIT Hyderabad

ICERM Workshop on Coding for Fault-Tolerant Computing
12th April, 2026

Joint Work with

Joint Work with
Shantom K. Borah, Abhinav Vaishya, Asit Kumar Pradhan, Bane Vasic
and Narayanan Rengaswamy

Motivation for Qudits

- Some systems are inherently higher dimensional problems
- Improved magic state distillation protocols
- Richer mathematical structure for code design

Pauli Group for Single Qudit

- Orthonormal basis for a single qudit Hilbert space is specified as,

$$\mathcal{B} = \{|\eta\rangle : \eta \in GF(q)\}.$$

$$X^a|x\rangle = |a + x\rangle, \qquad Z^b|x\rangle = e^{\frac{2\pi i}{p} tr(bx)}|x\rangle,$$

- The single qudit Pauli group for a q-dimensional system, where $q = p^m$, is defined as follows.

$$\mathcal{G}_q = \{e^{\frac{2\pi i}{p} x} X^a Z^b : x \in GF(p); a, b \in GF(q)\}$$

- Commutativity:

$$X^{x_1} Z^{z_1} X^{x_2} Z^{z_2} = e^{\left[\frac{2\pi i}{p} tr(z_1 x_2 - x_1 z_2)\right]} X^{x_2} Z^{z_2} X^{x_1} Z^{z_1}$$

  In particular, $X^{x_1} Z^{z_1}$ and $X^{x_2} Z^{z_2}$ commute if and only if $tr(z_1 x_2 - x_1 z_2) = 0$.
- Symplectic Representation: A qudit-Pauli operator $X^a Z^b \in \mathcal{G}_q$ is represented by the pair $[a|b] \in \mathbb{F}_q^2$.

Pauli Group for N Qudits

- Pauli group for a system of N qudits is the N-fold tensor product of the single qudit Pauli group and is denoted by $\mathcal{G}_q^{\otimes N}$.
- Symplectic Representation: A qudit-Pauli operator $X^{\underline{a}} Z^{\underline{b}} \in \mathcal{G}_q^{\otimes N}$ is represented by the pair $[\underline{a}|\underline{b}] \in \mathbb{F}_q^{2N}$.
- Commutativity of a subgroup: If the generators are represented in symplectic form in a matrix $\hat{S} = [A_x|A_z]$, the subgroup is commutative if and only if

$$tr(A_z A_x^T - A_x A_z^T) = 0.$$

Qudit Stabilizer Codes

- Stabilizer group $\mathcal{S}$, on a set of N qudits, is an Abelian subgroup of the N-fold Pauli group $\mathcal{G}_q^{\otimes N}$.
- Let $\langle S_1, S_2, \ldots S_M \rangle$ be a set of generators for $\mathcal{S}$.
- Stabilizer code $\mathcal{C}$ defined by $\mathcal{S}$ may then be defined as the subspace of the N-qudit Hilbert Space satisfying the condition,

$$S_i|\psi\rangle = |\psi\rangle \; \forall \; i = 1, 2, \ldots, M.$$

- True Stabilizer code:
  - S be a stabilizer group with symplectic representation $\hat{S}$. S is said to be "true", if $[x_P|z_P] \in \hat{S} \implies [\gamma x_P|\gamma z_P] \in \hat{S}, \forall \gamma \in \mathbb{F}_q$.
  - True stabilizer code is a code whose stabilizer group is "true".

Qudit CSS Codes

- CSS Code: Each generator S_i contains only X operators or only Z operators. The symplectic matrix for the stabilizer generators given by,

$$S = \left[\begin{array}{c|c} H_x & 0 \\ 0 & H_z \end{array}\right]; \quad tr(H_x H_z^T) = 0.$$

- "True" CSS codes are obtained from classical linear codes (otherwise additive codes in general)

Known Families of Qudit LDPC Codes

- Bivariate bicycle codes [STH+26]
- Hypergraph product codes [BPR+24, STH+26]
- La-cross [STH+26]
- Subsystem hypergraph product simplex codes [STH+26]
- High dimensional expander based codes [STH+26]
- Fiber bundle codes [STH+26]
- Lifted product codes [PK22] - codes constructed using non-abelian lifts and product expansion properties

Qudit Hypergraph Product Codes

- Let H_1 and H_2 denote the parity-check matrices of two classical codes over $\mathbb{F}_q$, with sizes $r_1 \times n_1$ and $r_2 \times n_2$.
- The hypergraph product of two classical codes $\mathcal{C}_1 = \ker(H_1)$ and $\mathcal{C}_2 = \ker(H_2)$ is defined as the quantum CSS code with check matrix

$$H = \begin{pmatrix} H_X & 0 \\ 0 & H_Z \end{pmatrix}$$

where $H_X = \begin{bmatrix} H_1 \otimes I_{n_2} & I_{r_1} \otimes H_2^T \end{bmatrix}$ and $H_Z = \begin{bmatrix} I_{n_1} \otimes H_2 & -H_1^T \otimes I_{r_2} \end{bmatrix}$.

Stacked Hypergraph Product Codes

Let $B_\alpha = \{\alpha_0, \alpha_1, \ldots, \alpha_{m-1}\}$ be the primal basis of $\mathbb{F}_q$ as a vector space over $\mathbb{F}_p$ and $B_\beta = \{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ be the trace-dual basis of B_α. Consider the stacking operators $\Omega_{\alpha,s}$ and $\Omega_{\beta,s}$ defined as follows:

$$\begin{aligned} \Omega_{\alpha,s} &= \begin{bmatrix} \alpha_0 & \alpha_1 & \ldots & \alpha_{s-1} \end{bmatrix}^T \\ \Omega_{\beta,s} &= \begin{bmatrix} \beta_0 & \beta_1 & \ldots & \beta_{s-1} \end{bmatrix}^T \end{aligned}$$

Let H_1 and H_2 denote the parity-check matrices of two classical codes over $\mathbb{F}_q$, with sizes $r_1 \times n_1$ and $r_2 \times n_2$ respectively. The stacked hypergraph product construction is given by the following matrices constituting the X-type and Z-type stabilizers:

$$\begin{aligned} H_X &= \Omega_{\alpha,s} \otimes H_x \\ &= \Omega_{\alpha,s} \otimes \begin{bmatrix} H_1 \otimes I_{n_2} & I_{r_1} \otimes H_2^T \end{bmatrix}, \\ H_Z &= \Omega_{\beta,s} \otimes H_z \\ &= \Omega_{\beta,s} \otimes \begin{bmatrix} I_{n_1} \otimes H_2 & -H_1^T \otimes I_{r_2} \end{bmatrix}. \end{aligned}$$

Bounds on Encoding Rate

Theorem

Let H_1, H_2 be two parity check matrices over $GF(q)$, where $q = p^m$ for some prime p. Then, the encoding rate $\mathcal{R}$ of the order-s stacked hypergraph product code obtained from these matrices is bounded as

$$\mathcal{R}_0 \leq \mathcal{R} \leq 1 - \frac{s}{m}(1 - \mathcal{R}_0),$$

where $\mathcal{R}_0 = \frac{k_1 k_2 + k_1^T k_2^T}{n_1 n_2 + r_1 r_2}$.

Bounds on Minimum Distance

- Minimum distance of fully stacked hypergraph product code

$$d \geq \min(d_1, d_2, d_1^T, d_2^T)$$

- Minimum distance of nonstacked hypergraph product code

$$d \geq \min\{w_1, w_2, w_1^T, w_2^T\},$$

where w_1 is the minimum weight of a non-zero vector such that $tr(H_1 c^T) = 0$. w_2, w_1^T and w_2^T are defined in a similar way.

- As stacking order increases, rate decreases and minimum distance increases.

$\mathbb{F}_q$-algebra

- $\mathbb{F}_q G$, where G is a group. The elements of $\mathbb{F}_q G$ are formal sums of the form $\sum_{g \in G} \alpha_g g$, where $\alpha_g \in \mathbb{F}_q$.
- Addition and multiplication can be defined.
- Left multiplication by a fixed element $\alpha \in \mathbb{F}_q G$ can be represented as a $\ell \times \ell$ matrix over $\mathbb{F}_q$, $\rho(\alpha)$ (where $\ell = |G|$).
- Elements of the group ring $R_\ell = \mathbb{F}_q[x]/(x^\ell - 1)$ can be represented as circulant matrices over $\mathbb{F}_q$.

Qudit Lifted Product Code

Let H_1 and H_2 be two matrices with entries from R_ℓ. Let $q = p^m$ and $1 \leq s \leq m$. Then, the order-s qudit lifted product code with respect to these two matrices is the qudit CSS code with H_x and H_z matrices given by,

$$H_x = \Omega_{\alpha,s} \otimes \rho \left(\begin{bmatrix} H_1 \otimes I_{n_2} & I_{r_1} \otimes H_2^T \end{bmatrix} \right),$$
$$H_z = \Omega_{\beta,s} \otimes \rho^* \left(\begin{bmatrix} I_{n_1} \otimes H_2 & -H_1^T \otimes I_{r_2} \end{bmatrix} \right),$$

where $\Omega_{\alpha,s}$ and $\Omega_{\beta,s}$ are the partial stacking operators and ρ is the matrix map (also same as lifting), applied element-wise to each entry in the above matrices. ρ^* is the conjugate map.

Tanner Code

- Ingredients:
  - Regular graph $\mathcal{G} = (V, E)$ with n vertices and vertex degree w.
  - Base code $\mathcal{C}_0$ over $\mathbb{F}_q$.

- Definition: $\mathcal{T}(\mathcal{G}, \mathcal{C}_0)$ is a wn length code obtained by indexing the edges of the graph with the coordinates of the code. The tanner code itself is defined by the following parity-check equations:

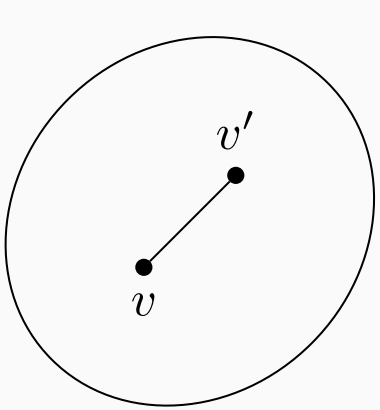
$$\forall \mathbf{c} \in \mathcal{T}(\mathcal{G}, \mathcal{C}_0), \forall v \in V, \mathbf{c}|_{N(v)} \in \mathcal{C}_0,$$

  where $N(v)$ denote the neighbors of v in $\mathcal{G}$.

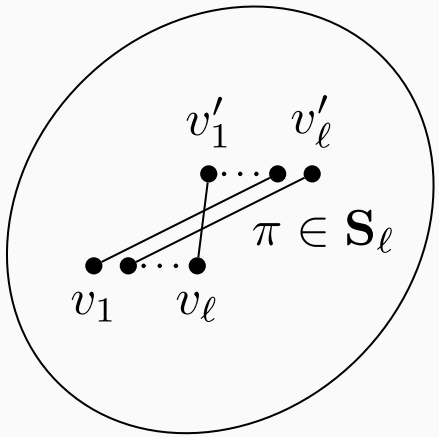
Cyclic Group Lift of a graph

Given a graph $\mathcal{G}$, ℓ-cyclic group lift of the graph is

- Replace each vertex in the graph with ℓ vertices.
- An edge between two vertices in $\mathcal{G}$ is replaced by ℓ edges between the two sets of ℓ vertices in the lifted graph.
- The ℓ edges themselves form a matching between the two sets of vertices, which is defined by the action of an element from the cyclic group $\mathbb{Z}_\ell$.



base graph G



ℓ-lift $\hat{G}$ of G

Qudit LP Code Construction

$H_1 = A$ and $H_2 = b = x - 1$. Denoted $\mathrm{LP}(A, x-1)$.
A and A^T are (α, β)-expanding. The following steps to construct A.

- **Step 1:** First ingredient of the construction is a code $\mathcal{C}_0$ over $\mathbb{F}_q$ such that the minimum distance of both the code $\mathcal{C}_0$ and $\mathcal{C}_0^{\perp}$ are good. Such codes can be found using a random coding argument.

- **Step 2:** Such a code is used as a local code in a Tanner code. Such a code has good minimum distance as well as low-weight parity checks too.

- **Step 3:** The above Tanner code is lifted through a process of cyclic group lift. The matrix $\rho(A)$ is given by the parity check matrix of this lifted Tanner code. A itself can be obtained from $\rho(A)$ through the inverse map.

Rate of Fully Stacked LP Code

- Dimension of the code in terms of matrix A is $\dim(\mathcal{C}(A(1)) + \dim(\mathcal{C}(A^T(1))$.
- A is $(m \times wn)$ matrix over R_ℓ.
- Length of the code is $N = \ell(wn + m)$.
  w is fixed. Thus, $N = O(\ell n)$.
- Dimension of the code is $O(n)$.

Minimum Distance of Fully Stacked LP Code

Theorem

Let $A \in \mathcal{M}_{m \times wn}(R_\ell)$ be a w-limited QC matrix such that A and A^{T} are (α, β)-expanding. Consider a lifted product code $\mathcal{Q} = \mathrm{LP}(A, x - 1)$. Then, $d(\mathcal{Q}) \geq \gamma\ell$, where γ is a constant depending on α, β and w.

- Minimum distance scales as $O(\ell)$.
- The product of rate and minimum distance scales as $O(\ell n)$ which is block length.
- Maximum possible minimum distance depends on the maximum ℓ (lift size) preserving the expansion property, which is exponential in n.

Core Idea of the Minimum Distance Proof

- Algebraic proof:
  - A codeword in $\mathcal{C}_Z$ satisfies $Au = (x-1)v$.
  - If the weight of u is small and non-zero, then the expansion property of A forces the weight of v to be large since the weight of $(x-1)v$ is atmost half that of v.
  - This core argument is used not directly for u and v but some "multiples" of u and v.

- Algorithmic proof:
  - Noisy syndrome decoding for the classical code with parity check matrix $\rho(A)$ is carried out.

Merged Syndrome Decoding

- Syndromes produced by the stabilizer measurements are in $GF(p)$ rather than $GF(q)$.
- Full stacked code

$$H_X = \begin{bmatrix} \alpha_0 H_x \\ \alpha_1 H_x \\ \vdots \\ \alpha_{m-1} H_x \end{bmatrix}; \qquad H_Z = \begin{bmatrix} \beta_0 H_z \\ \beta_1 H_z \\ \vdots \\ \beta_{m-1} H_z \end{bmatrix},$$

- Merging operation to get non-binary syndrome:

$$\tilde{s}_z = \sum_{i=0}^{m-1} s_{z,i}\beta_i = \sum_{i=0}^{m-1} tr(\alpha_i e_z \cdot H_x^T)\beta_i = e_z \cdot H_x^T$$

Simulation Results

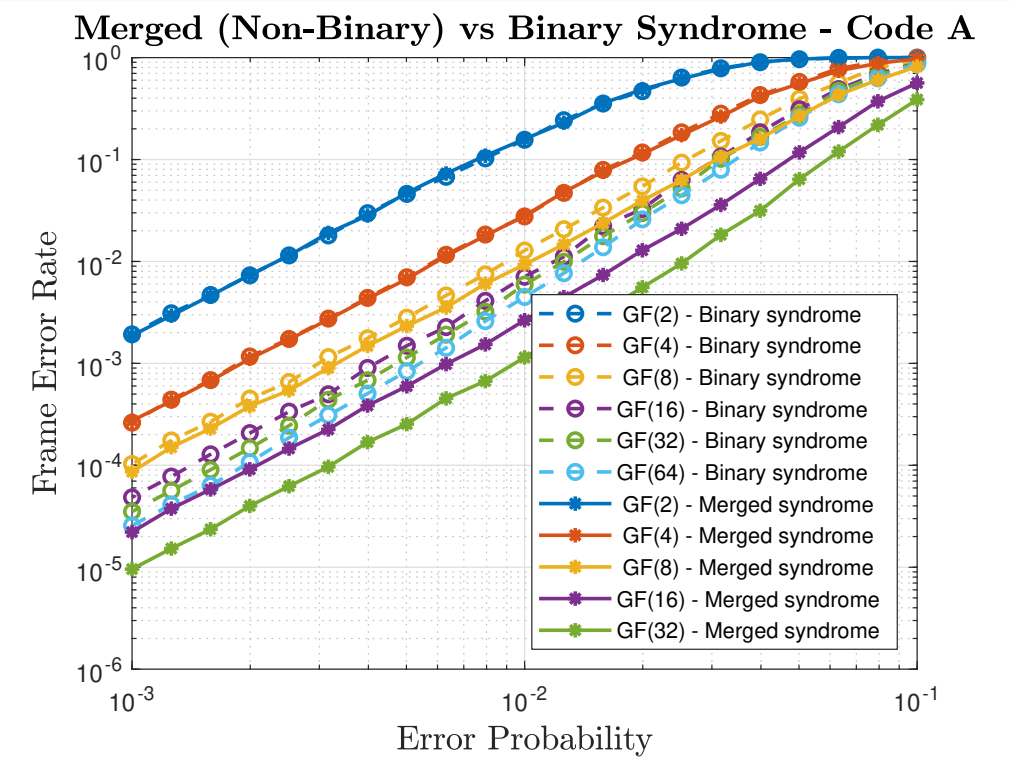


Figure 1: FER performance of code A, which is a fully stacked $[[320, 64]]$ hypergraph product code

Simulation Results

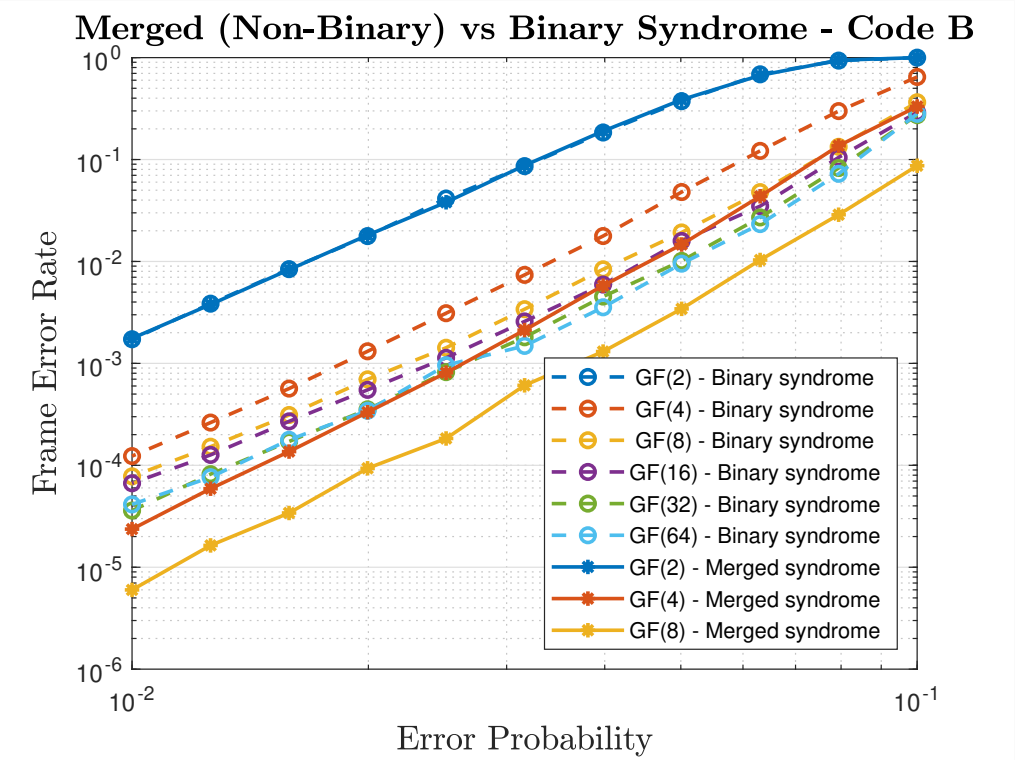


Figure 2: FER performance of code B, which is a fully stacked $[[900, 36, 10]]$ hypergraph product code

Simulation Results

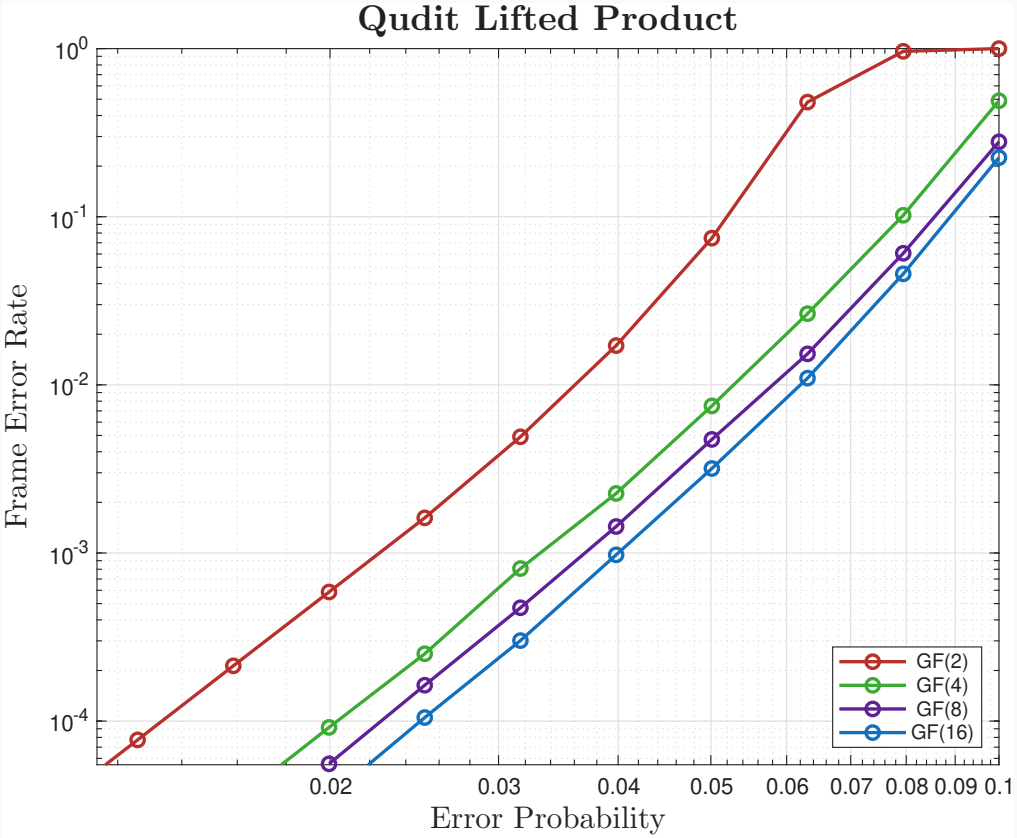


Figure 3: FER performance of C, which is a fully stacked $[[1054, 140, 20]]$ lifted product code

Open Problems

- For lifted product codes with general b, minimum distance proof.
- Say $b = 1 + x + x^3$ and ℓ is a multiple of 7.
- Tighter bounds on rate and distance for partially stacked codes.

References

- [PK21] Panteleev, Pavel, and Gleb Kalachev. "Quantum LDPC codes with almost linear minimum distance." IEEE Transactions on Information Theory 68, no. 1 (2021): 213-229.
- [PK22] Panteleev, Pavel, and Gleb Kalachev. "Asymptotically good quantum and locally testable classical LDPC codes." In Proceedings of the 54th annual ACM SIGACT symposium on theory of computing, pp. 375-388. 2022.
- [G24] Gottesman, Daniel. "Surviving as a quantum computer in a classical world," 2024.
- [BPR+24] Borah, Shantom K., Asit K. Pradhan, Nithin Raveendran, Narayanan Rengaswamy, and Bane Vasić. "Non-binary hypergraph product codes for qudit error correction." In IEEE International Conference on Quantum Computing and Engineering (QCE), 2024.

References

- [STH+26] Spencer, Daniel J., Andrew Tanggara, Tobias Haug, Derek Khu, and Kishor Bharti. "Qudit low-density parity-check codes." Quantum 2026.

- [NG21] Nadkarni, Priya J., and Shayan Srinivasa Garani. "$\mathbb{F}_p$-Linear and $\mathbb{F}_{p^m}$-Linear Qudit Codes From Dual-Containing Classical Codes." IEEE Transactions on Quantum Engineering 2 (2021): 1-19.

- [JMD+22] Jeronimo, Fernando Granha, Tushant Mittal, Ryan O'Donnell, Pedro Paredes, and Madhur Tulsiani. "Explicit Abelian Lifts and Quantum LDPC Codes." in 13th Innovations in Theoretical Computer Science Conference (ITCS 2022).

- [GG24] Golowich, Louis, and Venkatesan Guruswami. "Decoding quasi-cyclic quantum LDPC codes." in IEEE 65th Annual Symposium on Foundations of Computer Science (FOCS) 2024.